ASSEMBLEIA DA REPÚBLICA

Comissão para a Ética, a Cidadania e a Comunicação

EXMO. SENHOR
PRESIDENTE DA COMISSÃO DE ASSUNTOS EUROPEUS

Of. n.º 156/12ª/CPECC/2012 14-03-2012

Nº Único: 09.4

Assunto: Iniciativa Europeia: COM (2011) 163 Final

Para os devidos efeitos, junto envio a Vossa Excelência o Relatório relativo à COM (2011) 163 final - Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Proteção das infraestruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial», **aprovado por unanimidade, verificando-se as ausências do PCP e do BE,** na reunião desta Comissão Parlamentar realizada em **14 de março de 2012**.

Com os melhores cumprimentos,

O Presidente da Comissão,

(José Mendes Bota)

Palácio de S. Bento - 1249-068 LISBOA - PORTUGAL - Telefone: 21 391 96 55 - Fax: 21 391 75 08 - e-mail: Comissao.12A-CPECCXII@ar.parlamento.pt

ASSEMBLEIA DA REPÚBLICA

COMISSÃO PARA A ÉTICA, A CIDADANIA E A COMUNICAÇÃO

RELATÓRIO

Iniciativa Europeia: COM (2011) 163 Final

Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Proteção das infraestruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial»

1. Nota Introdutória

A Comissão Parlamentar dos Assuntos Europeus, em conformidade com o disposto no nº 1 do artigo 7º da Lei nº 43/2006, de 25 de Agosto, referente ao acompanhamento, apreciação e pronúncia pela Assembleia da República, no âmbito do processo de construção da União Europeia, remeteu à Comissão para a Ética, a Cidadania e a Comunicação, para esta se pronuncia sobre a matéria da sua competência, a COM (2011) 163 FINAL – COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES sobre a PROTECÇÃO DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO «REALIZAÇÕES E PRÓXIMAS ETAPAS: PARA UMA CIBERSEGURANÇA MUNDIAL».

A COM(2011)163FINAL dá conta dos resultados alcançados desde a adoção do Plano de Ação de Proteção das Infraestruturas Críticas da Informação (PICI)[1], em 2009, e descreve as etapas futuras a desenvolver tanto a nível europeu como a nível internacional, ao nível do reforço da segurança e da resiliência das ICI – Infraestruturas Críticas de Informação, não envolvendo qualquer iniciativa legislativa que implique a emissão de Parecer.

2. Enquadramento

[1] COM(2009) 149 que apresenta o Plano de Ação PICI - «Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência».

Como supra se referiu, a presente Comunicação tem por objeto o Plano de Ação PICI, destinado a reforçar a segurança e a resiliência das infraestruturas TIC – Tecnologias da Informação e Comunicação) vitais, que se insere numa estratégia global da União Europeia que visa a construção de um ambiente digital mais seguro.

Nesta estratégia inclui-se a Agenda Digital para a Europa[2], que elege, como um dos seus domínios-problema, a confiança e a segurança das tecnologias de informação, recomendando a *"aplicação rápida e eficaz do plano de ação da UE para a proteção das infraestruturas de informação críticas e do Programa de Estocolmo espoletará uma vasta gama de medidas no domínio da segurança das redes e da informação e do combate ao cibercrime. Por exemplo, para reagir em tempo real, deve ser criada na Europa, inclusivamente para as instituições europeias, uma rede ampla e funcional de equipas de resposta a emergências informáticas (CERT). A cooperação entre essas equipas e as entidades judiciais/policiais é essencial, pelo que seria útil promover um sistema de pontos de contacto para ajudar a prevenir o cibercrime e responder às emergências, como no caso de ciberataques. A Europa necessita igualmente de uma estratégia para a gestão das identidades, nomeadamente para que os serviços de governo eletrónico possam dar garantias de segurança e eficácia"*[3].

---

[2] COM (2010) 245. A Agenda Digital para a Europa constitui, por seu turno, uma das sete iniciativas emblemáticas da estratégia Europa 2020 e visa definir o papel que a utilização das tecnologias da informação e das comunicações (TIC) na concretização desta estratégia. O objetivo Agenda Digital para a Europa é definir um roteiro que maximize o potencial social e económico das TIC, com destaque para a Internet, um recurso fundamental da atividade económica e social: para os negócios, para o trabalho, para o lazer, para a comunicação e para a expressão livre das ideias.

[3] Para a concretização destes objetivos, a ADE estabelece as seguintes ações: Apresentação, em 2010, de medidas que visem pôr em prática uma política reforçada e de alto nível em matéria de segurança das redes e da informação, incluindo iniciativas legislativas, como a modernização da Agência Europeia para a Segurança das Redes e da Informação (ENISA), e outras medidas que permitam reagir mais rapidamente em caso de ataques informáticos, incluindo uma CERT para as instituições da UE; Apresentar, até 2010, medidas, nomeadamente iniciativas legislativas, que visem combater os ciberataques contra sistemas informáticos e, até 2013, regras em matéria de jurisdição do ciberespaço aos níveis europeu e internacional; Criar uma plataforma europeia para a cibercriminalidade até 2012; Até 2011, estudar a possibilidade de criar um centro europeu para a cibercriminalidade; Trabalhar com as partes interessadas a nível mundial, nomeadamente para reforçar a gestão mundial dos riscos na esfera digital e física e levar a cabo ações focalizadas, coordenadas a nível internacional, contra a criminalidade informática e os ataques à segurança; A partir de 2010, apoiar exercícios de preparação para a cibersegurança à escala da UE; No âmbito da modernização do quadro regulamentar da UE relativo à proteção dos dados pessoais25, que visa torná-lo mais coerente e capaz de oferecer maior segurança jurídica, estudar a possibilidade de extensão das disposições sobre notificação das violações da segurança; Até 2011, publicar orientações para a aplicação do novo quadro das telecomunicações no que respeita à proteção da privacidade dos indivíduos e dos dados pessoais; Apoiar a criação de pontos de denúncia de conteúdos ilegais em linha (linhas diretas) e campanhas de sensibilização sobre a segurança das crianças em linha conduzidas a nível nacional, e melhorar a cooperação pan-europeia e a divulgação das melhores práticas neste domínio; Promover o diálogo entre as várias partes interessadas e a auto-regulação dos fornecedores de serviços europeus e mundiais (por exemplo, plataformas de redes sociais, operadores de comunicações móveis), em especial no que respeita à utilização dos seus

De referir que em 2006 a União Europeia lançou o Programa Europeu de Proteção das Infraestruturas Críticas, que deu origem à Diretiva 2008/114/CE, transposta para o nosso ordenamento jurídico através do Decreto-Lei nº 62/2011, de 09 de Maio[4].

Já aqui se salientava[5] que esta Diretiva constituía *"a primeira etapa de uma abordagem faseada para identificar e designar as ICE [infraestruturas críticas europeias] e avaliar a necessidade de melhorar a sua protecção. Concentra-se, enquanto tal, nos sectores da energia e dos transportes, e deverá ser revista com o objectivo de avaliar o seu impacto e a necessidade de incluir no seu âmbito de aplicação outros sectores, designadamente o das Tecnologias da Informação e Comunicação (TIC)"*.

Em Março de 2009, a Comissão apresentou ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões a COM (2009) 149 - relativa à proteção das infraestruturas críticas da informação "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência".

Esta Comunicação centra-se na prevenção, preparação e sensibilização e define um plano de ações imediatas para reforçar a segurança e a resiliência das Infraestruturas Críticas de Informação e parte dos seguintes considerandos:

---

serviços por menores. Por outro lado, os Estados-Membros devem estabelecer, até 2012, uma rede funcional de CERT a nível nacional que cubra toda a Europa, efetuar, a partir de 2010, e em cooperação com a Comissão, operações de simulação de ataques em grande escala e testar estratégias de mitigação, pôr a funcionar em pleno, até 2013, as linhas diretas para denúncia de conteúdos em linha ofensivos ou prejudiciais, organizar campanhas de sensibilização sobre a segurança das crianças em linha, prever para as escolas disciplinas sobre segurança em linha e ainda incentivar os fornecedores de serviços em linha a implementarem medidas de auto-regulação no que respeita à segurança das crianças em linha; e, até 2012, criar plataformas nacionais de alerta ou adaptá-las à plataforma para o cibercrime da Europol.

[4] De acordo com o seu preâmbulo, *"O presente decreto-lei estabelece os procedimentos de identificação e de proteção das infra -estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes, transpondo a Directiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro. Com o presente decreto-lei, estabelecem-se procedimentos para a identificação das diversas infra -estruturas com funções essenciais para a sociedade, cuja perturbação ou destruição teria um impacto significativo, porque implicaria que essa infra -estrutura deixasse de poder assegurar essas funções. Assim, com o regime agora criado, Portugal adquire uma maior capacidade de intervenção ao nível da segurança e resiliência das infra -estruturas que venham a ser sectorialmente consideradas críticas, no âmbito europeu, integrando o futuro Programa Europeu de Protecção de Infra - estruturas Críticas (PEPIC) suportado numa abordagem transversal dos riscos a que essas infra – estruturas possam estar expostas"*.

[5] Ponto 5 do Preâmbulo da Diretiva.

- As tecnologias da informação e das comunicações (TIC) são uma parte vital da economia e da sociedade europeias;

- São, em geral, considerados infraestruturas críticas da informação, já que a sua perturbação ou a sua destruição teria um forte impacto nas funções vitais da sociedade.

- Os ciberataques atingiram um nível de sofisticação sem precedentes e estão a transformar-se numa actividade sofisticada lucrativa ou ditada por motivos políticos; Os ciberataques em grande escala contra a Estónia, a Lituânia e a Geórgia são os exemplos mais amplamente conhecidos de uma tendência geral. A enorme quantidade de vírus, vermes e outras formas de malware, a expansão das botnets (redes de computadores zombies) e o aumento contínuo do spam confirmam a gravidade do problema;

- Em 2008, o Fórum Económico Mundial calculou que a probabilidade de ocorrer uma ruptura importante nas ICI nos próximos 10 anos era de 10 a 20%, com um potencial custo económico global de cerca de 250 000 000 000 USD;

- Por outro lado, os processos e as práticas de monitorização e comunicação de incidentes de segurança das redes variam significativamente de Estado-Membro para Estado-Membro. Em alguns deles não existe uma organização de referência que funcione como ponto de monitorização. Mais significativa ainda é a aparente insuficiência da cooperação e da partilha, entre os Estados-Membros, de dados fiáveis e operáveis sobre incidentes de segurança, partilha essa que é informal ou se limita a um intercâmbio bilateral.

Nesta Comunicação, a Comissão refere-se igualmente à Resolução º 58/199 da Assembleia Geral da ONU sobre a criação de uma cultura mundial de cibersegurança e a protecção das infraestruturas críticas da informação e a recente recomendação da OCDE sobre a protecção das infra-estruturas críticas da informação.

Em conformidade, a COM (2009) 149 define cinco pilares de ação, nomeadamente a **preparação e prevenção** a todos os níveis, **deteção e resposta**, através da criação de mecanismos adequados de alerta rápido, a **mitigação e recuperação**, reforçando os mecanismos de defesa das ICI na UE, a **cooperação internacional**, promovendo internacionalmente as prioridades da EU e a definição de **critérios para o sector das TIC**, através da aplicação da diretiva relativa à identificação e designação das infra-estruturas críticas europeias.

É a avaliação das medidas propostas para cada um destes pilares e a definição de acções para o futuro que é objecto da COM(2011) 163 Final.

De referir que sobre esta matéria, em termos de legislação, existe uma proposta de Diretiva do Parlamento e do Conselho, de 20 de Setembro de 2010, relativa a ataques contra os sistemas de informação[6], justificada pela necessidade de intervenção da União Europeia neste domínio, pela necessidade de criminalizar certas formas de infrações não incluídas na atual Decisão-Quadro, em especial as novas formas de ciberataque, e ainda pela necessidade de eliminar obstáculos às investigações e ações penais nos processos transfronteiras[7].

3. Análise

Como supra se referiu, a COM(2011)163Final visa identificar os resultados alcançados desde a adoção do Plano de Ação PICI, descreve as etapas previstas para cada ação, tanto a nível europeu como internacional, e procura intensificar a cooperação entre os Estados-Membros e o sector privado aos níveis nacional, europeu e internacional.

Adota-se no presente relatório a metodologia de exposição utilizada na presente Comunicação.

3.1. Um Cenário em Evolução

A COM(2011)163Final dá conta da "*dependência social, política e económica da Europa em relação às TIC, mas também o crescimento constante do número, âmbito, sofisticação e impacto potencial das ameaças – sejam elas naturais ou de origem humana*", salientando o surgimento de novas ameaças tecnologicamente mais sofisticadas, verificando-se "*uma tendência para a utilização das TIC na conquista de predomínio político, económico e militar, nomeadamente através das suas capacidades*

---

[6] E que vem revogar a Decisão-Quadro 2005/222/JAI do Conselho.

[7] A proposta de Diretiva assinala que: "*A principal causa da cibercriminalidade é a vulnerabilidade resultante de vários factores. Uma resposta insuficiente dos mecanismos de aplicação da lei contribui para a prevalência destes fenómenos e agrava as dificuldades, já que certos tipos de crimes têm carácter transfronteiriço. As denúncias relativas a este tipo de crime são muitas vezes inadequadas, em parte porque alguns crimes não são detectados e em parte porque as vítimas (operadores económicos e empresas) não os denunciam por temerem que a exposição pública das suas vulnerabilidades afecte a sua reputação e as perspectivas comerciais futuras. Além disso, as diferenças entre as legislações e procedimentos penais nacionais podem dar origem a diferenças a nível da investigação e das acções penais, conduzindo a discrepâncias no tratamento dado a estes crimes. A evolução no domínio das tecnologias da informação exacerbam estes problemas, facilitando a produção e distribuição de instrumentos («malware» e «botnets») e proporcionando ao mesmo tempo anonimato aos infractores e dispersando a responsabilidade por várias jurisdições. Dadas as dificuldades em levar a cabo uma acção penal, a criminalidade organizada consegue obter lucros consideráveis com riscos reduzidos. A presente proposta tem em conta os novos métodos utilizados para cometer cibercrimes, nomeadamente o recurso aos* «botnets»".

ofensivas. A «ciberguerra» ou o «ciberterrorismo» são por vezes mencionados neste contexto".

A Comunicação agrupa as ameaças em três tipologias:

- As que têm por finalidade a exploração, como as «ameaças avançadas persistentespara fins de espionagem económica e política (por exemplo, GhostNet), o roubo de identidades, os recentes ataques ao sistema de comércio de emissões[8] ou os ataques contra os sistemas TI dos Estados;

- As que têm por finalidade introduzir perturbações, como os ataques de Recusa Distribuída de Serviço ou "spamming" gerado via "botnets" (por ex., a rede Conficker de 7 milhões de máquinas e a rede Mariposa, com base em Espanha, de 12,7 milhões de máquinas), a Stuxnet e o corte de meios de comunicação;

- As que têm por finalidade a destruição. Trata-se de um cenário ainda não materializado, mas que não pode ser de todo excluído no futuro, dada a crescente presença das TIC nas infra-estruturas críticas (como as redes eléctricas e os sistemas de abastecimento de água inteligentes).

3.2. A União Europeia e o contexto mundial

A COM(2011)163FINAL dá conta de que não é possível, em matéria de tecnologias de informação e comunicação efetuar uma abordagem europeia, , sendo necessário envidar esforços no sentido de uma *gestão mundial de riscos*.

3.3. A aplicação do Plano de Ação PICI

A Comunicação destaca as principais ações realizadas no âmbito do Plano de Ação, destacando os progressos efetuados, no campo da preparação e prevenção, no âmbito do Fórum Europeu de Estados-Membros (EFMS), nomeadamente *"na promoção do debate e da troca de pontos de vista entre as autoridades competentes sobre boas práticas políticas em matéria de segurança e de resiliência das infra-estruturas TIC"*, sendo que as futuras atividades do EFMS irão incidir *"na cooperação entre as equipas de resposta a emergências informáticas (CERT) nacionais/governamentais, com vista a definir os incentivos económicos e regulamentares à segurança e à resiliência (no*

[8] Ver Q&A em: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

respeito das regras aplicáveis em matéria de concorrência e de auxílios estatais), avaliar o estado da cibersegurança na Europa, promover exercícios pan-europeus e discutir as prioridades da concertação internacional a nível da segurança e da resiliência".

Destaca-se igualmente a relevância das equipas de resposta a emergências informáticas (CERT), a nível nacional, e que, em cooperação com a ENISA (Agência Europeia para a Segurança das Refes e da Informação), se constitua *"uma rede de CERT nacionais/governamentais totalmente operacionais em todos os Estados-Membros até 2012. Essa rede constituirá a espinha dorsal de um sistema europeu de partilha de informações e de alerta (SEPIA ou, na sigla inglesa, EISAS) para os cidadãos e as PME, que será construído até 2013 com recursos e capacidades nacionais".*

Ao nível da deteção e resposta, salienta-se o facto de a ENISA ter elaborado *"um roteiro de alto nível para o desenvolvimento do sistema SEPIA até 2013, alicerçado na implementação de serviços básicos ao nível das CERT nacionais/governamentais e de serviços de interoperabilidade, para que os sistemas nacionais de partilha de informações e de alerta sejam integrados no SEPIA. A proteção adequada dos dados pessoais será um dos elementos fundamentais desta atividade".*

No campo da mitigação e recuperação, destaca-se a relevância da realização de exercícios de resposta a ataques informáticos, enquanto em matéria de cooperação internacional se comete à Comissão a discussão e promoção *"com as partes interessadas relevantes, em particular o sector privado (através da parceria EP3R), bilateralmente com os principais parceiros internacionais, em particular os EUA, e também a nível multilateral. Fá-lo-á, no âmbito das suas competências, em fóruns como o G8, a OCDE, a NATO (nomeadamente com base no seu novo Conceito Estratégico, adoptado em Novembro 2010, e nas actividades do Cooperative Cyber-defense Center of Excellence), a UIT (no contexto da criação de capacidades no domínio da cibersegurança), a OSCE (por intermédio do seu Fórum para a cooperação em matéria de segurança), a ASEAN, o Meridian[9], etc. O objectivo é transformar estes princípios e orientações num quadro comum que propicie o empenho colectivo internacional em assegurar a resiliência e a estabilidade a longo prazo da Internet".*

Finalmente, assinala-se, ao nível dos critérios para as definição de infraestruturas críticas europeias em matéria das TIC, a conclusão de uma "primeira versão de critérios específicos para o sector das TIC a aplicar na identificação das infra-estruturas

[9] O processo Meridian visa dotar os governos de todo o mundo de um meio através do qual possam discutir o modo de cooperar a nível das políticas no que respeita à protecção das infra-estruturas críticas da informação (PICI). Ver http://meridianprocess.org/

críticas europeias, incidindo mais em particular nas comunicações fixas e móveis e na Internet".

3.4. Próximas etapas

A Comissão destaca os resultados positivos alcançados na execução do Plano de Ação PICI e elege, como tarefa prioritária, a promoção de um "cultura mundial de gestão de riscos", definindo, para esse efeito, a elaboração de princípios para a resiliência e a estabilidade da Internet, a construção de parcerias estratégias internacionais e a promoção da confiança na informática em nuvem.

Em simultâneo, exorta os Estados-Membros a *"melhorar o estado de preparação da UE, criando, até 2012, uma rede de equipas CERT nacionais/governamentais totalmente operacionais. Na mesma linha, as instituições da UE criarão também uma CERT ao seu nível até 2012. Todos estes esforços deverão tirar partido do conjunto mínimo de capacidades e serviços básicos e das recomendações políticas conexas, elaborados pela ENISA, que continuará a fornecer o seu apoio a estas iniciativas. Esta acção irá também acelerar o desenvolvimento, até 2013, de um sistema europeu de partilha de informações e de alerta (SEPIA) para o grande público"*.

Apela igualmente aos Estados-Membros para conceberem *"um plano de emergência europeu em caso de incidente informático, até 2012, e organizar exercícios pan-europeus regulares no domínio da cibersegurança. Os exercícios no domínio da cibersegurança são um elemento importante de uma estratégia coerente de planeamento da resposta a emergências e das acções de recuperação em caso de incidentes informáticos tanto ao nível nacional como europeu. Os futuros exercícios pan-europeus no domínio da cibersegurança deverão basear-se num plano de emergência europeu para incidentes informáticos que tire partido e se articule com os planos de emergência nacionais. Tal plano deverá prever os mecanismos e procedimentos de base para as comunicações entre Estados-Membros e, igualmente importante, contribuir para a definição do âmbito e para a organização dos futuros exercícios pan-europeus. A ENISA trabalhará com os Estados-Membros na elaboração desse plano europeu de emergência para incidentes informáticos, que deverá estar pronto até 2012. Nesse mesmo prazo, todos os Estados-Membros deverão elaborar planos nacionais de emergência e prever exercícios de resposta e de recuperação"*.

4. Síntese

A presente Comunicação, ao dar conta das ações efetuadas no âmbito do Plano de Ação PICI e das etapas futuras, alerta igualmente para uma matéria particularmente sensível ao nível da segurança e progresso da União Europeia e dos seus cidadãos face à ameaça, real, de ataques informáticos cujas consequências podem ser insuportáveis a todos os níveis.

5. Conclusões

Face ao exposto, a Comissão para a Ética, a Cidadania e a Comunicação, delibera:

- Tomar conhecimento da COM(2011)163 Final - Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Proteção das infraestruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial»;

- Remeter o presente relatório à Comissão de Assuntos Europeus;

- Remeter o presente relatório à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, para conhecimento.

Palácio de São Bento, 14 de Março de 2012

A Deputada Relatora

(Isabel Oneto)

O Presidente da Comissão

(José Mendes Bota)